48048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of : **AFEK et al.**

Serial No.: 09/929,877 : Group Art Unit: 2151

Filed : August 14, 2001 : Examiner: Frantz B. Jean

For : METHODS AND APPARATUS FOR PROTECTING AGAINST OVERLOAD CONDITIONS ON NODES OF A DISTRIBUTED NETWORK

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

DECLARATION UNDER 37 CFR 1.131

Sir:

We, the undersigned, Yehuda Afek, Anat Bremler-Barr and Dan Touitou, hereby declare as follows:

1) We are the Applicants in the patent application identified above, and are the inventors of the subject matter described and claimed in claims 1-8, 10, 11, 13-16, 20, 33, 35 and 46-69 therein.

2) We conceived our invention prior to September 28, 2000, in Israel, a WTO country. We were then diligent in preparation of a provisional patent application covering the

invention during the period between September 28, 2000, and October 17, 2000, when the provisional patent application (US 60/240,899) was filed. The present patent application (US 09/929,877) claims priority from this provisional patent application.

3) As evidence of the conception of the present invention, we attach hereto, as Exhibits A and B, parts of a draft of the present patent application. These documents were prepared September 14, 2000, and September 18, 2000, respectively. (Proof of the dates of these documents, as well as other documents cited herein, is attached hereto as Exhibit G in the form of a directory listing of the archive in which the documents were stored. The relevant files and dates in the archive are noted below.)

4) The following tables show the correspondence between the independent claims now pending in this application and Exhibits A and B. In view of this correspondence, it is clear that we conceived the claimed invention prior to September 28, 2000.

Claim 1	**Exhibits**
A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network	Exhibit A, page 1, paragraph 1: "NetGuard system is activated upon receiving alerts of an attack. The system than focused on defending only the victim(s) of the attack."

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

A. responsively to an indication of an anomalous traffic condition, initiating diversion of traffic destined for the victim by a first set of one or more network elements external to the set of one or more potential victims to a second set of one or more network elements external to the set of one or more potential victims	Exhibit A, page 1, paragraph 4: "At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard. This is done by routing any traffic using the *victim public address* to NetGuards. Hence achieving our first goal, that traffic to the victim, from outside the network, and inside the network, is redirected to NetGuards."
B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim.	Exhibit A, page 1, last paragraph: "The NetGuards machine, discriminates between traffic to the victim that is part of the attack, and genuine traffic. The traffic of the attack would be blocked at NetGuards. Genuine traffic would be routed from the NetGuards to the victim, using the *victim private address*."

Claim 46	**Exhibits**
A network element for use in protecting against an overload condition on a network	Exhibit A, page 1, paragraph 1: "NetGuard system is activated upon receiving alerts of an attack. The system than focused on defending only the victim(s) of the attack."

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

an input for receiving traffic diverted from the network, the traffic comprising flows of data packets having respective source addresses	Exhibit A, page 1, paragraph 4: "At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard. This is done by routing any traffic using the *victim public address* to NetGuards." Exhibit B, section 1.1: "It is common (e.g., in the Cisco convention) to define a network flow by the following parameters: i. Source IP address…"
a statistics module that is arranged to perform a statistical analysis of the diverted traffic so as to detect an anomalous pattern of a flow associated with at least one of the source addresses	Exhibit B, section 1.3.2: **"Attack Analysis**: Will be conducted during attack time and will be responsible to compare the historically collected statistical data with the current traffic volume and generate rules for traffic blockage. The output of this unit, in general, will consist of a list of items for each of which three parameters will be provided: a. **Network flow**, identified by a combination of source IP address (can be prefixed), destination IP address, destination port number, protocol type…"

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

a filter, which is operative, responsively to detection of the anomalous pattern, to block at least a portion of the data packets having the at least one of the source addresses	Exhibit B, section 1.3, last paragraph: "The analysis will be based on the statistical parameters of the data and will aim at keeping the attacked destination at normal loads by blocking the most 'suspected' traffic streams."
an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter	Exhibit A, page 1, last paragraph: "The NetGuards machine, discriminates between traffic to the victim that is part of the attack, and genuine traffic. The traffic of the attack would be blocked at NetGuards. Genuine traffic would be routed from the NetGuards to the victim, using the *victim private address*."

Claim 46	**Exhibits**
A system for use in protecting against an overload condition on a network	Exhibit A, page 1, paragraph 1: "NetGuard system is activated upon receiving alerts of an attack. The system than focused on defending only the victim(s) of the attack."
one or more network elements ("guards") disposed on the network	Exhibit A, page 1, paragraph 4: "At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard."

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

an input for receiving traffic from the network	Exhibit A, page 1, paragraph 4: "This is done by routing any traffic using the *victim public address* to NetGuards."
a filter coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition	Exhibit B, section 1.3, last paragraph: "The analysis … will aim at keeping the attacked destination at normal loads by blocking the most 'suspected' traffic streams."
a statistics module that is coupled to the filter and that identifies the traffic statistically indicative of having originated from the source suspected as potentially causing the overload condition	Exhibit B, section 1.3.2: "**Attack Analysis**: Will be conducted during attack time and will be responsible to compare the historically collected statistical data with the current traffic volume and generate rules for traffic blockage. The output of this unit, in general, will consist of a list of items for each of which three parameters will be provided: a. **Network flow**, identified by a combination of source IP address (can be prefixed), destination IP address, destination port number, protocol type…"

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter	Exhibit A, page 1, last paragraph: "The NetGuards machine, discriminates between traffic to the victim that is part of the attack, and genuine traffic. The traffic of the attack would be blocked at NetGuards. Genuine traffic would be routed from the NetGuards to the victim, using the *victim private address*."
one or more further network elements ("diverters") disposed on the network and in communication with the guards, the further network elements selectively initiating, responsively to detection of an anomalous traffic condition, diversion to at least one of the guards traffic otherwise destined for a still further network element ("victim") in a set of one or more potential victims on the network	Exhibit A, page 1, "routers" shown in the figure diverting traffic to "NetGuards," as stated in paragraph 4 on page 1: "At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard. This is done by routing any traffic using the *victim public address* to NetGuards. Hence achieving our first goal, that traffic to the victim, from outside the network, and inside the network, is redirected to NetGuards."

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

Claim 56	Exhibits
A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network	Exhibit A, page 1, paragraph 1: "NetGuard system is activated upon receiving alerts of an attack. The system than focused on defending only the victim(s) of the attack."
diverting to a guard machine traffic destined for the victim, the traffic comprising flows of data packets having respective source addresses	Exhibit A, page 1, paragraph 4: "At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard. This is done by routing any traffic using the *victim public address* to NetGuards." Exhibit B, section 1.1: "It is common (e.g., in the Cisco convention) to define a network flow by the following parameters: ii. Source IP address…"

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

performing a statistical analysis of the diverted traffic at the guard machine so as to detect an anomalous pattern of a flow associated with at least one of the source addresses	Exhibit B, section 1.3.2: "**Attack Analysis:** Will be conducted during attack time and will be responsible to compare the historically collected statistical data with the current traffic volume and generate rules for traffic blockage. The output of this unit, in general, will consist of a list of items for each of which three parameters will be provided: a. **Network flow,** identified by a combination of source IP address (can be prefixed), destination IP address, destination port number, protocol type…"
a filter, which is operative, responsively to detection of the anomalous pattern, to block at least a portion of the data packets having the at least one of the source addresses	Exhibit B, section 1.3, last paragraph: "The analysis will be based on the statistical parameters of the data and will aim at keeping the attacked destination at normal loads by blocking the most 'suspected' traffic streams."

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

responsively to detecting the anomalous pattern, preventing at least a portion of the data packets having the at least one of the source addresses from reaching the victim while passing to the victim at least some of the data packets from other source addresses	Exhibit A, page 1, last paragraph: "The NetGuards machine, discriminates between traffic to the victim that is part of the attack, and genuine traffic. The traffic of the attack would be blocked at NetGuards. Genuine traffic would be routed from the NetGuards to the victim, using the *victim private address*."

Claim 66	**Exhibits**
A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network	Exhibit A, page 1, paragraph 1: "NetGuard system is activated upon receiving alerts of an attack. The system than focused on defending only the victim(s) of the attack."
coupling the victim to receive traffic from the network via a first port of a network switch	Exhibit A, page 1: In the figure, the victim is coupled to receive traffic via one output of a router.

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

actuating the network switch to divert the traffic destined for the victim to a second port to which a guard machine is coupled	Exhibit A, page 1, paragraph 4: "At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard. This is done by routing any traffic using the *victim public address* to NetGuards." The figure shows that the NetGuard is coupled to a different port of the router from the victim.
filtering the diverted traffic using the guard machine	Exhibit A, page 1, last paragraph: "The NetGuards machine, discriminates between traffic to the victim that is part of the attack, and genuine traffic. The traffic of the attack would be blocked at NetGuards."
selectively passing at least a portion of the filtered traffic from the guard machine to the victim	Exhibit A, page 1, last paragraph: "The traffic of the attack would be blocked at NetGuards. Genuine traffic would be routed from the NetGuards to the victim, using the *victim private address*."

5) During the period between September 28 and October 17, we worked continuously and diligently to revise and supplement the material in the original drafts in order to complete the provisional patent application that was subsequently filed. Some of the draft documents that we prepared during this period are attached hereto as Exhibits C, D, E and F. These documents were completed, respectively, on September 29, October 2, October 9, and October 13, 2000. We then

completed and filed our provisional patent application on October 17, 2000.

6) Exhibit G is a directory listing of the archive from which Exhibits A-F were taken. The table below lists the file names and dates as they appear in Exhibit G:

Exhibit	File Name	Date
A	Netxxn.doc	September 14, 2000
B	Statistical-patent4.doc	September 18, 2000
C	Copy of netxx.doc	September 29, 2000
D	Attack Identification.doc	October 2, 2000
E	Statistical-patent-hanoch5	October 9, 2000
F	Mordi.ppt	October 13, 2000

US 09/929,877

Declaration under 37 C.F.R 1.131 by Afek et al.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application of any patent issued thereon.

Yehuda Afek
Citizen of Israel
26 Hacarmel Street
Hod Hasharon
Israel

Date:

Anat Bremler-Barr
Citizen of Israel
17 Hashomron Street
Ramat Hasharon
Israel

Date: 11/9/08

Dan Touitou
Citizen of Israel
21 Golani Street
Ramat Gan 52224

Israel

Date: